REMARKS

I. Introduction

In response to the Office Action dated May 24, 2004, claims 1, 2, 6, 8, and 32 have been amended. Claims 1-37 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. The Cited References and the Subject Invention

A. The Wasilewski Reference

U.S. Publication No. 2001/0046299, published November 29, 2001 to Wasilewski et al. disclose an authorization of services in a conditional access system. A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

B. The Colligan Reference

U.S. Patent No. 6,415,031, issued July 2, 2002 to Colligan et al. disclose a selective and renewable encryption for secure distribution of video on-demand. Selective encryption is provided in a process which includes: determining whether a predetermined criterion is satisfied; setting a selective encryption status field if the predetermined criterion is satisfied; and encrypting an unencrypted payload to generate an encrypted payload, and constructing a packet with the encrypted

payload, if the predetermined criterion is satisfied. The predetermined criterion may be one of several criteria, each of which reduce the required amount of encryption and decryption while maintaining a high level of security. Renewable encryption is provided in a process which includes: copying a first encrypted digital video program from a remote server to a video source; decrypting the first encrypted digital video program using a first key to generate an unencrypted digital video program; encrypting the unencrypted digital video program using a second key to generate a second encrypted digital video program; transmitting the second encrypted digital video program from the video source to the remote server; and deleting the first encrypted digital video program from the remote server.

IV. Office Action Prior Art Rejections

In paragraphs (2)-(3), the Office Action rejected claims 1-37 under 35 U.S.C. § 103(a) as unpatentable over Wasilewski, U.S. Publication No. 2001/0046299 (Wasilewski) in view of Colligan et al., U.S. Patent No. 6,415,031 (Colligan). Applicants respectfully traverse these rejections

With Regard to Claims 1 and 25: Claim 1 recites:

> *A method of storing program material for subsequent replay, comprising the steps of:*
> *receiving a data stream in a receiver having a storage device, the data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;*
> *further encrypting the encrypted program material according to a second encryption key;*
> *encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and*
> *storing the further encrypted program material and control data and the fourth encryption key in the storage device.*

Note that the Applicants have amended claim 1 to recite that the data stream is received in a receiver having a storage device and that the further encrypted storage material is stored in the storage device. These amendments are made to clarify the context of the Applicants invention. It is noted that these amendments include subject matter that was recited in claim 6, and hence, should not require a new search.

According to the Office Action,

> "Wasilewski discloses a method and apparatus for protecting the transfer of data comprising the steps of receiving a data stream comprising the program material (Figure 2A, clear MPEG-2 program) encrypted according to a first encryption key (Figure 2A, element 201) and control data (Figure 2A, element 203), the control data comprising the first encryption key (Figure 2A, element 202) and being encrypted (Figure 2A, element 204) and encrypting the second encryption key according to a third encryption key to produce a fourth encryption key (Figure 2A, elements 205-207) and storing the further encrypted program material and control data and the fourth encryption key (page 4, paragraph 0062)."

The Applicants respectfully disagree. As best the Applicants can ascertain, the Office Action argues that the Applicants' invention is obvious because one of ordinary skill in the art would modify FIG. 2A of the Wasilewski reference as follows:

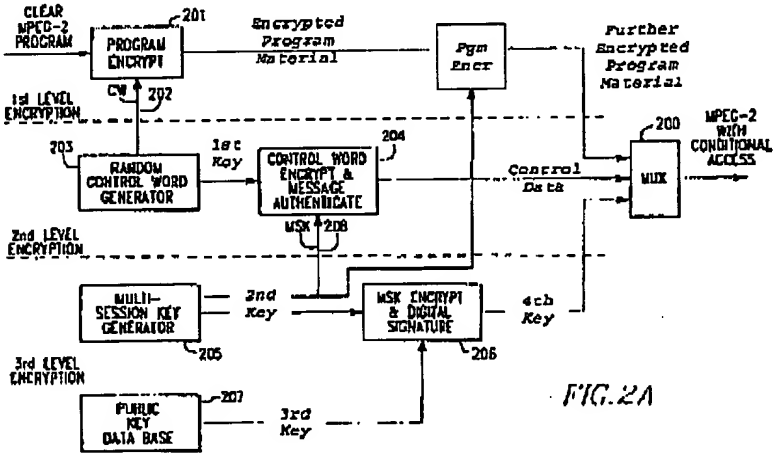

FIG. 2A

But in this paradigm, there is no entity that *receives a data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted* as claim 1 requires. Under the Office Action's proposed modification, the input to the

mux 200 is two separate data streams, not one data stream, and one of those data streams is a *further encrypted program material and control data.*

So, then, perhaps, the encryption module should be located thusly:

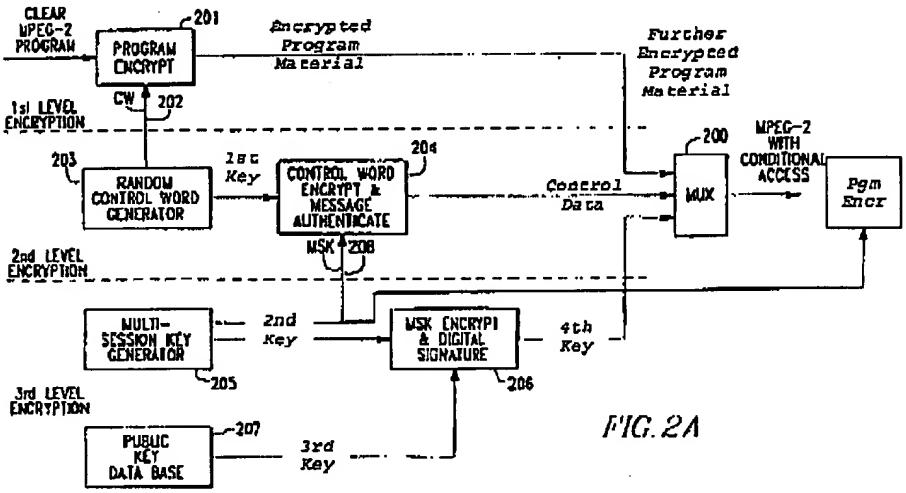

FIG. 2A

But that would also encrypt the 4th key with the 2nd key, a result that does not make sense, because the 4th key was generated *from* the 2nd key. The receiver could therefore not decrypt the 4th key with the 3rd key to obtain the 2nd key. Essentially, the apparatus would be non-operational. The problem with the Office Action's analysis of FIG. 2A is two-fold:

First, blocks 205-206 are not analogous to the step of *encrypting the second encryption key according to a third encryption key to produce a fourth encryption key* as recited in claim 1. Instead, block 205 is a process that generates a key (MSK) that is used to encrypt the control word (which control word is used to encrypt the program). That key encrypted with the subscriber's public key (using asymmetric encryption) and subscriber so that the subscriber can decrypt the CW, and use the decrypted CW to decrypt the program. These operations are similar to those that are described on page 11 of the Applicants disclosure (except that the Applicant's system describes the encryption and decryption of the CW as performed using an I/O indecipherable algorithm), and are not analogous to the step of *encrypting the second key according to the third encryption key to produce a fourth encryption key.*

Second, the Wasilewski and Colligan references, even when combined, do not teach the basic paradigm of the Applicants' invention ... that of receiving a transmitted datastream in a receiver and securely storing that received datastream. Wasilewski indeed teaches storing in paragraph [0062], but that storage is a form of transmitting the program material to the viewer ... it is an alternative to the step of receiving datastream transmitted from the head end:

> [0062] .... Also, the transmission medium may be storage media, where the service origination point is the manufacturer of the media, and the service reception component may be the element which reads the storage media. For example, the transmission medium can be a CD-ROM, DVD, floppy disk, or any other medium that can be transferred, physically, electronically, or otherwise.

Neither Wasilewski or Colligan disclose *receiving a data stream in a receiver having a storage device, the data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted* and storing the program material and control data in the storage device, let alone after *further encrypting the encrypted program material according to a second encryption key* and *encrypting the second encryption key according to a third encryption key to produce a fourth encryption key.*

In rejecting claim 6 (which previously recited that the datastream is received in a *receiver*), the Office Action relied on the following:

> [0059] In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1.sup.st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be -combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208).

> [0060] The MSK 208 has a longer lifetime than CW 202. The MSK lifetime is typically hours to days in length. MSK 208 is both encrypted and digitally signed by MSK Encrypt & Digital Signature function 206 before being sent to MUX 200 encapsulated EMM 111. MSK 208 and other parts of EMM 111 are preferably encrypted using a public key algorithm, such as the well-known RSA algorithm, with a public key associated with the specific set-top box 113 to which the EMM is addressed. The public keys of all set-top boxes 113 in a system 101 are stored in Public Key Data Base 207. The public keys in this data base are preferably certified by a certificate authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In the case of an RSA digital signature, the private key which is used to make the signature belongs to the entitlement agent within service distribution organization 103 responsible for authorizing the associated service.

While the foregoing discloses a set-top box receiving a signal, it is not the signal described in claim 1, and it does not precede the storing step recited in claim 1. Simply put, the Office Action has taken the foregoing disclosure out of context with the remainder of Wasilewski, and this feature out of context with the rest of claim 1.

Finally, the Applicants respectfully disagree that there is any teaching to combine the Wasilewski and Colligan references. According to the Office Action, one of ordinary skill in the art would modify Wasilewski as described in Colligan to "strengthen the security for the distribution of program material for subsequent replay." However, Wasilewski itself teaches that triple DES can be applied to the program to increase security:

> [0095] .... The information needed by the entitlement agent is forwarded entitlement information 417; to ensure the privacy of the customer, this information is encrypted using the 3DES algorithm with a key 420, as shown at 343, to produce encrypted forward entitlement information 419. The key 420 is composed of two 56-bit DES keys. The 3DES encryption operation is a sequence of three DES operations: encryption using the first DES key, decryption using the second DES key, and encryption using the first DES key Then key 420 is encrypted using the public key 335 of the entitlement agent and the scaled digest is made using the private key of DHCT 333. All of these parts together make up forwarded purchase message 421, which is addressed to the entitlement agent.

Colligan teaches a multi-layer encryption, but Colligan teaches that the multi-layer encryption is used to reduce the cost and storage requirements for fully encrypting the program before sending it to the user:

> Unlike distribution of digital cable television channels, distribution of digital video on-demand (VOD) follows a pointcast model in that the content is transmitted from a video server to each individual viewer. Due to the nature of pointcasting, a security scheme for digital VOD which is based on the model provided by security for cable television broadcasts would be impractical and expensive. **First, fully encrypting the digital VOD in real-time every time the digital video is transmitted from the server to an individual viewer is quite expensive in both cost and space usage for encryption equipment.** (col. 2, lines 49-59, emphasis added)

Such concerns are not relevant in the context of the Applicants invention, as the process of further encryption is performed by the subscriber's equipment (upon a *received* datastream). For the foregoing reasons, the Applicants cannot agree that there is any teaching to modify Wasilewski as described in Colligan.

Claims 23, 24, and 25 recites features analogous to those of claims 1, respectively, and are patentable on the same basis.

With Respect to Claim 2 and 26: Claim 2 recites:

> *The method of claim 1, further comprising the steps of:*
> *retrieving the stored further encrypted program material, control data and the fourth encryption key from the storage device;*
> *decrypting the fourth encryption key using the third encryption key to produce the second encryption key;*
> *decrypting the further encrypted program material with the second encryption key to produce the encrypted program material;*
> *decrypting the control data to produce the first encryption key; and*
> *decrypting the encrypted program material using the first encryption key.*

Claim 2 recites the features of claim 1, and is patentable on the same basis. Claim 1 also recites features related to decryption that render it even more remote from the cited references. The Office Action does not indicate where such steps are disclosed in the Wasilewski or Colligan references.

Claim 26 recites features analogous to those of claim 2 and is patentable on the same basis.

With Respect to Claim 16: Claim 16 recites:

> *A receiver for storing program material for subsequent replay, comprising:*
> *a tuner, for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key;*
> *a first encryption module, communicatively coupled to the tuner and communicatively coupleable to a media storage device, for further encrypting the encrypted program material according to a second encryption key and for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;*
> *a first decryption module communicatively coupleable to the media storage device, for decrypting the fourth encryption key retrieved from the media storage device using the third encryption key to produce the second encryption key, and for decrypting the further encrypted program material retrieved from the media program device to produce the encrypted program material;*

a conditional access module communicatively coupled to the first decryption module, for decrypting the encrypted access control information to produce the first encryption key; and

a second decryption module, for decrypting the program material using the first encryption key.

The Office Action does not indicate where Wasilewski and/or Colligan reference disclose any of the foregoing features. For example, even if the mux 200 shown in FIG. 2A of the Wasilewski reference can be said to receive *a data stream comprising encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key* as described in claim 1, it is not received by a *tuner*. Other features are similarly missing, including, for example a conditional access module, and a decryption module.

With Respect to Claims 3, 4, 19-20, 27, and 28: Claim 3 recites:

The method of claim 2, further comprising the steps of:

accepting a PPV request before decrypting the encrypted program material using the first encryption key; and

recording billing information regarding the program material.

According to the Office Action, this is disclosed as follows:

Broadcast Events

[0228] A broadcast event is a one-time service, such as a pay-per-view broadcast of a boxing match. In the preferred embodiment, there are two kinds of broadcast events: ordinary pay-per-view broadcast events, in which the customer has ordered in advance to see the event, and impulse events where the customer decides at the time the event is broadcast that he wants to order it. There are different kinds of impulse events, such as: impulse pay-per-view (IPPV) events, which are pay-per-view events where the customer can decide at the time of the event to purchase it, and near video-on-demand (NVOD), where popular movies are rebroadcast at short intervals and the customer can decide when the rebroadcast occurs whether he or she wants to view it. Those skilled in the art will realize that the concept of an "event" can refer to any service over a specific time period (whether broadcast or non-broadcast), such as video on demand events or other types of events not listed here.

[0229] In the case of pay-per-view events, the customer orders the event from the entitlement agent, and the agent responds by sending an EMM that contains the necessary entitlement information. In the case of events where the customer decides at broadcast time that he or she wants to purchase the event, purchase information, i.e., information about the entitlements that can be purchased, must be distributed with the event. In these cases, the purchase information is distributed by means of global broadcast authenticated messages, or GBAMs. The customer provides input 628 that specifies a purchase. The DHCT 333 responds to the input 628 by storing the record of purchase in the DHCTSE 627 and then beginning to decrypt the event. Later, the DHCT 333 sends the entitlement agent a forwarded purchase message (FPM) indicating what has been purchased by the customer, and the entitlement authority responds with an EMM that confirms the purchase

> and contains the necessary entitlement information. The record of the purchase remains until an EMM confirming the purchase is received by the DHCTSE 627.

However, recalling that the Office Action argued that the step of *storing the further encrypted program material and the control data and the fourth encryption key in the storage device* was disclosed only as an alternative to an ordinary broadcast transmission:

> [0062] .... Also, the transmission medium may be storage media, where the service origination point is the manufacturer of the media, and the service reception component may be the element which reads the storage media. For example, the transmission medium can be a CD-ROM, DVD, floppy disk, or any other medium that can be transferred, physically, electronically, or otherwise.

it is wholly inappropriate to ignore that teaching and argue that Wasilewski teaches both the storage described in claim 1 and the accepting of a PPV request before decrypting the encrypted program material that is described in claim 3. Accordingly, the Applicant respectfully traverses the rejection of claim 3 as well.

Claim 19 recites the features of claim 16 and is patentable on that basis alone. Claim 19 also recites that the first encryption module further encrypts the encrypted access control information according to the second encryption key. In other words, unlike claim 16, *both* the encrypted program material *and* the access control information are further encrypted. There is no teaching in Wasilewski or Colligan to further encrypt *both* the encrypted program material and the encrypted access control information. Further, this would appear to require modification of FIG. 2A as follows:

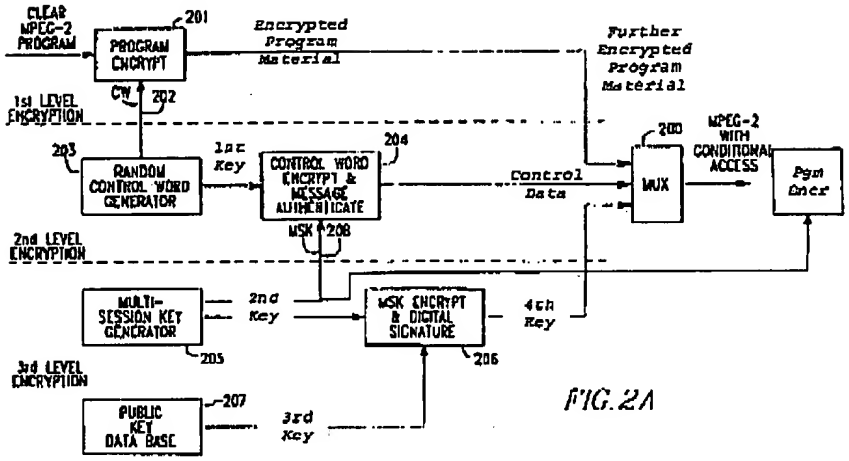

FIG. 2A

and as described above, that would render the system inoperable (the second key could not be obtained).

Claims 4 and 28 recite analogous features and are patentable on the same basis.

With Regard to Claims 6, 7, 21, and 30-31: Claim 6 recites that the third key is unique to the receiver, and claim 7 recites that the second key is unique to the receiver. According to the Office Action, these features are disclosed as follows:

> [0059] In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1.sup.st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be -combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208).
>
> [0060] The MSK 208 has a longer lifetime than CW 202. The MSK lifetime is typically hours to days in length. MSK 208 is both encrypted and digitally signed by MSK Encrypt & Digital Signature function 206 before being

> sent to MUX 200 encapsulated EMM 111. MSK 208 and other parts of EMM 111 are preferably encrypted using a public key algorithm, such as the well-known RSA algorithm, with a public key associated with the specific set-top box 113 to which the EMM is addressed. The public keys of all set-top boxes 113 in a system 101 are stored in Public Key Data Base 207. The public keys in this data base are preferably certified by a certificate authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In the case of an RSA digital signature, the private key which is used to make the signature belongs to the entitlement agent within service distribution organization 103 responsible for authorizing the associated service.

However, this is plainly not the case. Referring back to the rejection of claim 1, the second key is the key that is used to further encrypt the data stream after it is received. Since the Office Action admits that Wasilewski does not teach the further encrypting with the second key step, the foregoing cannot teach the second key or that the second key is receiver unique.

In essence, the problem with the rejection is that it confuses which key is which, and where and in which order the operations are being performed. The foregoing merely discloses the use of a public/private key pair used by the set-top box and the service distribution organization (SDO). Even with respect to the third key, the foregoing teaches only the use of a key pair ... it does not teach, expressly or inherently that the receiver key be unique.

With Respect to Claims 12-14 and 36: Claim 12 recites that the second encryption key is derived at least partially from metadata describing program material replay rights. According to the Office Action, this is disclosed as follows:

> [0059] In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1.sup.st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be -combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208).

Again, the Applicants respectfully disagree. The foregoing refers to what the Office Action analogizes as the first encryption key and the third encryption key, not the second encryption key. Colligan was said to disclose the use of the second encryption key to further encrypt the encrypted program. How then, can the foregoing portion of the Wasilewski reference disclose deriving that key from metadata? And how can the foregoing disclose deriving a second encryption key from the broadcast time when the second encryption key itself is not disclosed?

Further, as far as the Applicants can ascertain, the foregoing does not disclose generating any key from metadata describing program material replay rights, or at least partially from the broadcast time of the program material.

With Respect to Claims 15 and 37: Claim 15 recites the features of claims 1, 11, 12, 13, and 14, and also recites features in which the PPV request is permitted or not based upon the stored portion of metadata. The Office Action suggests that these features are disclosed as follows:

> [0061] In FIG. 2B, the corresponding DHCT private key and associated DHCT public secure micro serial number are stored in memory 232 of decoder 240. Public secure micro serial number is provided so that demultiplexer 230 can select an encrypted multi-session key addressed to decoder 240 from transport data stream (TDS). Encrypted multi-session key E.sub.Kpr (MSK) is decrypted in decryptor 234 using DHCT private key from memory 232 to provide multi-session key MSK. Demultiplexer 230 also selects from transport data stream TDS encrypted control word (CW) E.sub.MSK (CW). The encrypted CW is processed in decryptor 236 using multi-session key MSK as the decryption key to provide the unencrypted CW. The unencrypted CW preferably changes at a high rate, for example, once every few seconds. Demultiplexer 230 also selects from transport data stream TDS encrypted service E.sub.CW (SERVICE). The encrypted service is processed in decryptor 238 using the CW as the decryption key to recover the unencrypted service.
>
> [0097] A global broadcast message is one which is not addressed to any individual DHCT 333 or to any group of DHCTs 333. In a preferred embodiment, global broadcast messages accompany instances of services and contain information that is relevant to the instance they accompany. Consequently, the encryption and authentication techniques used in the global broadcast messages must permit rapid decryption and authenticity checking. One example of a global broadcast message is the ECM. Other examples are the different types of global broadcast authenticated messages, or GBAMs. As with ECMs, it is necessary to prevent global broadcast messages from being spoofed, and it is done in the same fashion as with the ECMs. More specifically, the digest is made using some or all of the MSK together with the content of the global broadcast message. The MSK thus functions as a shared secret between the entitlement agent and DHCT 333. When EMM manager 407 receives the global message, it makes a digest using the contents of the received message and the MSK and responds to the received message only if the digest agrees with the one contained in the message. An advantage of using a digest made with the MSK to authenticate the global broadcast message is that the digest may be both made and checked very quickly.
>
> [0126] DHCTSE 627 stores keys, interprets EMMs and ECMs, and produces FPMs. With the EMMs and ECMs, it does the decryption and authentication required for interpretation and with FPMs, it makes the sealed digest and encrypts the FPM. Thus, in the preferred embodiment, EMM manager 407 is implemented in secure

element 617. In addition, DHCTSE 627 provides encryption, decryption, digest, and digital signature services for other applications executing on DHCT 333. Secure element (DHCTSE) 627 includes a microprocessor and memory that only the microprocessor may access. Both the memory and the microprocessor are contained in tamper-proof packaging. In interpreting EMMs, DHCTSE 627 acquires and stores keys and entitlement information; in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services. DHCTSE 627 further records purchase information for impulse-purchasable services such as IPPV and stores the purchase data securely until the data is successfully forwarded via a forwarded purchasing message to control suite 607. DHCTSE 627 maintains MSK for the EAs, the private/public key pairs for DHCT 333, and the public keys of the conditional access authorities and the entitlement agents.

and

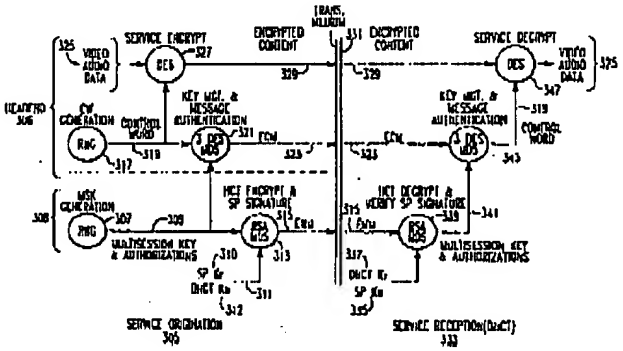

FIG. 3

As the Applicants do not understand what element the Office Action analogizes to metadata and the second key derived at least in part from that metadata, the Applicants do not understand how the foregoing discloses the features described in claims 15 and 37 (and again, this is made difficult by the fact that the Office Action itself admits that the foregoing does not disclose a second key). The Applicants respectfully suggest that a more specific explanation would be helpful to understand this rejection.

With Respect to Claim 22: Claim 22 recites that the first encryption module and the first decryption module are implemented in a single chip device. According to the Office Action, it is quite well known in the art to perform encryption/decryption operations in a single chip. However, this is not true in the present case, as the Wasilewski reference does not disclose a single entity that

would include the first encryption module and the first decryption module. The first encryption module is that entity that further encrypts the encrypted program material, but the first decryption module is the entity that decrypts the fourth encryption key. Even assuming that Wasilewski could be modified as shown in Colligan, that would mean that the first encryptor and the first decryptor would be in different entities. Accordingly, the rejection of claim 22 is traversed as well.

V. Dependent Claims

Dependent claims 2-15, 17-22, and 26-37 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VI. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: August 24, 2004

By: _____
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/amb